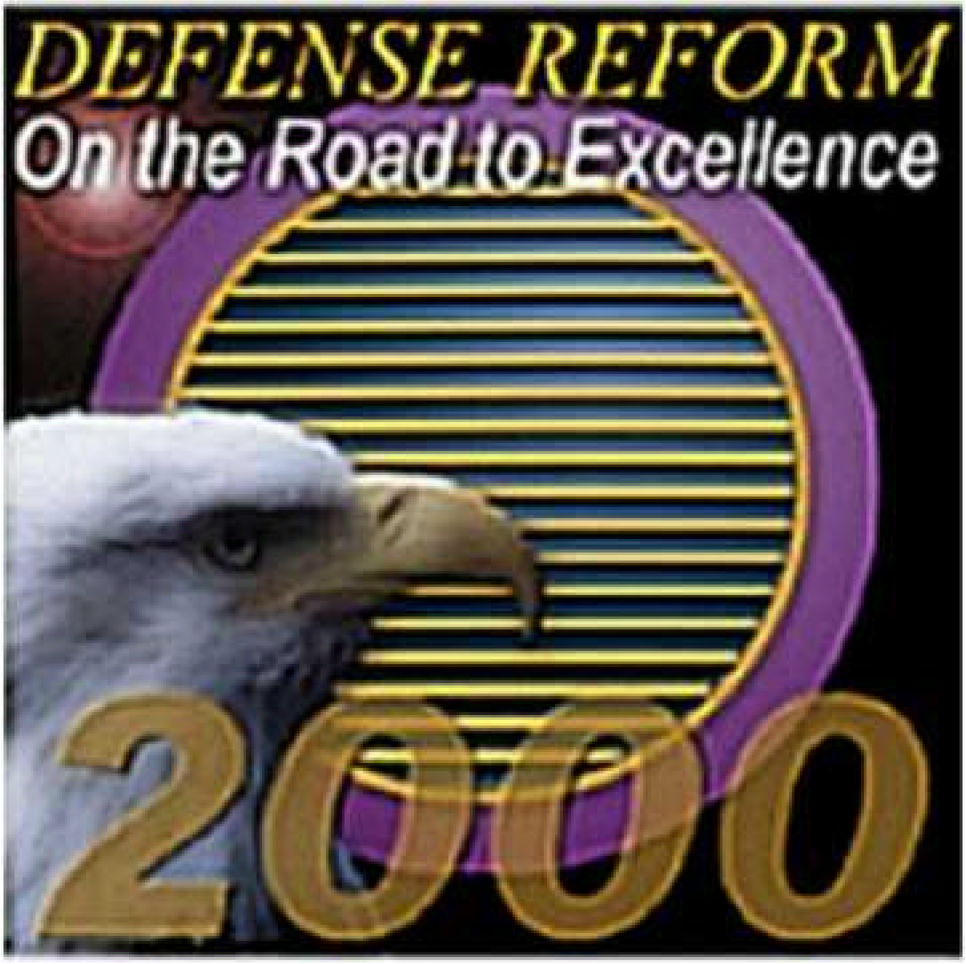

Electronic Commerce Conference
People Barrier's Sub-Group
Issue Paper

The common denominator is clear: People are the weakest link in any security model, for technology alone will not be the “silver bullet” that insures information protection. The human factor must be dealt with through regular, ongoing training and awareness initiatives. While people are the primary safeguard, they are also the greatest potential threat to security.

Who are these "people?" They are systems and network administrators, other IT professionals, users of systems, contractors, and in particular, the decision-makers and senior policy leaders both inside and outside the cyber community. Everyone must be aware and yet, according to a 1999 Information Security Industry Survey, 35% of industry respondents do not believe that information security has high visibility within their respective organization. **See Attachment 1, Table 1, Infosecurity Visibility.** Over 85 percent of all respondents say security has improved at their organization over the past two years, and 95 percent are confident it will improve even more by 2001. But in light of the less-than-reassuring facts about the state of security—breaches continue to cost each organization hundreds-of-thousands of dollars each year—such optimism may be misinformed.

Conducted in April and May 1999, the 1999 Industry Survey was completed by 745 Information Security readers, a pool of respondents that includes administrators, managers and executives in IT, security, networking and data management. The survey jointly sponsored by ICSA TruSecure (www.icsa.net) and Global Integrity Corporation (www.globalintegrity.com) had the goal to assess the state of information security from the perspective of those responsible for it and to pinpoint the obstacles to enterprise security. It also was intended to gauge the pervasiveness and effectiveness of commercial security products and to drill down into the increasing problems associated with security breaches.

IV. Problem Statement

Systems are currently under unprecedented attack, with intensity certain to increase over time. The question is how to safeguard systems, and how best to achieve information assurance given the human factors barriers. Too often people are unaware of best security practices or employ practices that fail to make sense. These are human-related management concerns, not technical issues. The majority of people typically do not think of security implications during their day-to-day activities and annual awareness programs will do little to stem this practice and make daily awareness the norm rather than the exception. Four percent of the respondents in the 1999 Information Security Industry Survey stated that they did not even know whether their organization had a security policy and 20% said their organization did not have a security policy in place. Ominously, these organizations represent the critical dependency that DoD increasingly shares with the nation's infrastructure. **See Attachment 1, Table 2, Policy By Industry.** Often overlooked according to Dorothy Denning, professor of Computer Science at Georgetown University in Washington DC, and author of "Information Warfare and Security," is that the most effective defense against cyber threats, real or imagined, is "an educated public that understands the issues and the threats involved." (Source: National Defense, February 2000) An educated public must be 100% aware of any security policies for which they are responsible.

Users of Federal computers all need continuing education and training to remain abreast of developments in information systems technology and understand how to best protect the contents of those information systems. Unfortunately, no coordinated Federal Government effort exists to teach computer ethics or rules of behavior to employees working on Federal computer systems. DoD has always imposed on its personnel requirements for maintaining appropriate security. Although such requirements have covered practices in information security, there are at present no criteria that an individual can be said to meet or not to meet. Thus, for all practical purposes, enforcement of information security requirements has not been possible, according to a March 1999 statement by a spokesperson for the Defense Information Assurance Program.

A 1996 survey of Federal agencies and private corporations is illustrative in showing the trend that few employees even had a working knowledge of current laws on the misuse of computer systems. **See survey results in Attachment 2, Figure 1.** For agencies to meet the critical issue of training, the Office of Technology Assessment noted that automated courses on computer ethics and safeguarding would allow large numbers of government employees to receive training more cheaply than through traditional classrooms. The Computer Security Act of 1987 requires agencies to improve security and protect privacy of sensitive information on Federal computer systems. Although it mandates training as a means of attaining improved security awareness and accepted computer security practices, the Act does not address agency budgetary resources so that in reality the training provision of the 1987 Act is an inadequately funded mandate.

V. Discussion

Preparing the IA workforce for cyber security is more than a process or a program; it is a way of life. Given this formidable challenge, a proven way to achieve acceptable levels of security is though a concerted program of security awareness, training and education for all users and administrators. Regrettably, training priorities are often low, and are too frequently the "first to go" in response to time or funding constraints. Changing this entrenched frame of mind will require behavior modification (cultural change) across all levels of workforce.

Recent studies affirm ongoing training activities are important in mitigating the "people" problem, but these studies affirm that training effectiveness and current training activities are largely outmoded, inadequate and poorly implemented. An obvious conclusion: training for training sake is not working. But what type of training and how much is enough? Currently, easily applied metrics for measuring of security training adequacy are lacking.

The Computer Security Institute (CSI) announced in March 2000 the results of its fifth annual Computer Crime and Security Survey. Conducted in cooperation with the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, the survey is intended to raise the level of security awareness, as well as help determine the scope of computer crime in the United States. Trends evidenced in recent years are disturbing: cyber crimes and other information security breaches are widespread and diverse. Ninety percent of respondents reported cyber attacks, many of which can result in serious damages. The 273 organizations able to quantify the attacks reported losses exceeding $265 million. Unfortunately, no dollar figure is calculable for federal losses due to cyber-terrorism from which to derive a return on security investment. Clearly, more investment is needed in terms of adherence to sound practices, deployment of sophisticated technologies, and most importantly adequate staffing and training of information security practitioners in both the private sector and government.

Federal/DoD agencies must have adequate resources to support IA security training efforts to respond to emerging threats and correct known vulnerabilities through new training courses, accelerated training schedules, and by innovative multimedia delivery methods. Development of CBT and web-based IA training packages, for example, that are customized for senior management, IT practitioners, and cyber users are effective ways for introducing technology to help mitigate user diversity.

There exists a serious shortage of qualified trainers. Officials need to assess hiring practices, training, and development of the DOD IT/IA workforce. An assertive refreshment/awareness program is needed to systematically upgrade IA skills of the current workforce in light of the burgeoning need. The IA learning curve must begin at new employee orientation and continue regularly, preferably daily, for all employees at all levels of command. The need for an aggressive awareness program for senior DOD IT managers is vital for ensuring a continued understanding and appreciation of the criticality of implementing a robust IA adherence program within an organization.

Industry budgets for Information Security are increasing. According to the July 1999 Information Security Industry Survey, the average organizational security budget increased 21.7 percent from 1998 to 1999. Estimates for growth from 1998 to 2000 show a 26.6 percent increase in organizations spending more than $500K on security, a forecast affecting nearly a fifth of all respondents. **See Attachment 2, Figure 2.**

While budgets continue to increase across the public and private sectors, those working in the security trenches continue to feel cash-strapped. Overall, just one-third of respondents from the July 1999 Information Security Industry Survey felt security budgets were sufficient. **See Attachment 1, Table 3, Are Budgets Keeping Up?** While almost half of those in the high tech/computing field were satisfied with security funding, a meager 18 percent of security professionals in the education field agreed with their budget. In fact, nearly two out of three respondents – 63 percent of the overall sample – said lack of budget was an impediment to protecting data and resources within their organization, up from 58 percent in the 1998 sample. When asked to name the single greatest obstacle to security, more than twice as many respondents pointed to "budget constraints" than to any other security deterrent. **See Attachment 2, Figure 3.**

The July 1999 Information Security Industry Survey, shows that most respondents—83 percent overall—are pleased with the level of management support/awareness in their organizations. **See Attachment 1, Table 4, Organizational Awareness.** While survey respondents are mostly happy with management, they are less pleased with the user community's support and IA awareness. Only 55 percent said end-users support information security needs, according to the survey. The problem is most pronounced in the manufacturing/distribution vertical, where only 40 percent of respondents said end-users are supportive of information security.

Awareness, too, is all-important. In announcing the new Senate's Critical Infrastructure Protection Working Group (CIP) on March 27, 2000, Senator Bob Bennett of Utah, Chairman of the Senate Republican High Tech Task Force who will chair the new working group stated, "The interconnectivity and advanced capabilities of U.S. computer systems makes the United States more vulnerable to cyber attacks than any other nation in the world. Such attacks could bring the U.S. economy to its knees. To prepare to meet this threat, CEO's and CIO's must be made aware of its severity and have access to the most up-to-date, comprehensive information available."

VI. Alternatives

Enhanced security instruction can best be achieved using cyber teaching methods. Among the alternative means for promoting and implementing IA awareness are outsourcing, traditional military training organizations, and web-based development solutions. The Web-based alternative offers the best trade-off for cost-effective performance while minimizing the impact on overtaxed military educational resources. Similarly, alternatives for delivering instruction include traditional classroom, stand-alone self-study, and web-based learning. Again, the web-based alternative is preferred due to anytime, anywhere availability and the helpful multimedia feature that promotes instructional possibilities and improves student comprehension.

VII. Recommendations

The following recommendations reinforce and complement improvements now underway within the Defense Department, and are intended to streamline successful cyber-security implementation.

1. **Implement an aggressive, broad-based awareness program.** Awareness is applicable across the enterprise, embracing not only the IT professional, but the users and managers as well. IA orientation is essential for all that use or apply information services. Moreover, the transient nature of the DoD workforce underscores the need for continuous reinforcement of sound security practices at all levels to mitigate the 'weak link' syndrome. Personal security responsibility should be combined with enforceable consequences of non-compliance. Lastly, outreach worldwide with the commercial community to share information and knowledge and best practices, can be used to incorporate these lessons learned into on-line training programs.
2. **Create a one-stop shop IA repository and establish a single DoD coordinator to capture best practices and facilitate information collection and use.** Centralized information sharing is essential to organize and enhance awareness, particularly since defense organizations inherently have common problems and solutions, and are increasingly reliant on each other's infrastructure. A central coordinator will collect pertinent IA information for distribution and develop a model agreement for cross-sector sharing. A series of tailored messages to each audience (leadership, supervisor, system admin specialist or user) will increase awareness effectiveness.
3. **Provide adequate funding to mount an aggressive awareness and training campaign.** Security improvement must be matched with the requisite resources and realistic priorities to empower those having the responsibility to conduct and carry forward IA awareness and training programs. The DoD CIO, working with the Comptroller, should identify the resources and develop Defense Program Guidance language to require

funding for workforce training. To overcome the present shortage of qualified trainers, additional funding to resolve this deficiency should be earmarked as a top priority.

4. **Implement Smart Training Techniques.** Use technology wherever possible to leverage security-training methods. Distance learning and distributed learning techniques provide a cost-effective, continuous learning media that can be used for cyber training of active duty and reservists, anyplace, anytime. Promote web-enabled learning options using audio/video products, webcast and websites to reach target audiences and to interact with the vast DoD audience. Instead of annual security lectures, make training "fun" and based on "live" or "real life" scenarios that can be injected into daily work environments. Finally, solicit universities and private sector national experts to play a pivotal role in developing the IT/IA workforce by contributing to training partnerships across government, industry and academia. For example, establish a virtual IA classroom/academy as a forum to enhance IA skills using webcast or distance learning techniques and featuring the world's foremost IA experts as facilitators/instructors to further strengthen 'student' use of this virtual global resource.
5. **Direct DoD CIO to expand their effort to develop and require security engineering professionalism courses and certificate programs.** Develop a professionalism program complete with tests, degrees, and technical competence certificates. Educational programs should take into consideration curriculum development at the undergraduate and graduate levels. The National Defense University curriculum should be expanded to ensure that program managers implement integrated Information Assurance throughout the life cycle of critical systems and programs. On-the-job training is an important element of the overall training program, and should be augmented with more formal training leading to certification of information security professionals. Establish a procedure for routine evaluation of Agency/Service/Department training program effectiveness through established oversight programs and by independent evaluators. Make IA training an integral part of DOD personnel performance evaluations. Finally, establish incentives to encourage implementation of security guidelines.
6. **Develop and use metrics for measuring the success of IA education, training, and awareness programs.** It is currently difficult locating statistics and significant data about the personnel performance improvements occurring as a result of any IA awareness or training programs. Developing metrics and using them to measure the degree of cultural changes occurring within the way people "think" security will be useful for determining the most efficient use of training techniques and awareness programs.
7. **Further study and analysis should be performed to evaluate IA awareness implications of IT professionals and untrained employees.** A paucity of hard evidence exists regarding the business risk inherent in maintaining a workforce inadequately trained about security. Validated official studies would prove invaluable in setting future budget priorities supporting awareness and training activities.

VIII. Implementation Concerns

A number of factors contribute toward successful implementation of the above recommendations. These factors include funding, leadership, technology availability, management buy-in, time to accomplish, methods on how to train the masses, and how to instigate training across stovepipe organizations.

Cultural factors are at play inhibiting change within the workforce. One challenge is how to instill in people the need to "think security" another is to consider risk when using internet resources, and a third, how to better accept responsibility for infrastructure protection and integrate security into individual's daily activities.

IX. Resource Implications

The principal factor that weighs on security is funding. Inadequate training budgets, low funding priorities and competition for resources with other activities are among the realities facing every organization, and must be overcome or mitigated through concerted management attention. Early investment in training will reduce overall costs.

Issue Paper: People Barrier’s to Information Assurance

Table 1: Infosecurity Visibility

Overall, does infosecurity have high visibility within your organization?

Industry	Yes	No
Aerospace (n=24)	83%	17%
Banking/Financial (n=92)	70%	30%
Communications/Telecom (n=41)	61%	39%
Consulting (n=81)	64%	36%
Education (n=40)	45%	55%
Government (n=129)	66%	34%
High-Tech/Computer* (n=112)	73%	25%
Insurance/Real Estate/Legal (n=32)	59%	41%
Manufacturing/Distribution (n=53)	38%	62%
Medical/ BioTech (n=30)	53%	47%
Military (n=32)	81%	19%
Other* (n=32)	70%	29%
OVERALL (n=745)	**65%**	**35%**

Table 2: Policy By Industry

Does your organization currently have a security policy?

Industry	Yes	No	Don't Know
Aerospace	96%	4%	0%
Banking/Financial	84%	14%	2%
Communications/Telecom	68%	22%	10%
Consulting	69%	25%	6%
Education	55%	40%	5%
Government	79%	16%	5%
High-Tech/Computer	75%	22%	3%
Insurance/Real Estate/Legal	81%	19%	0%
Manufacturing/Distribution	67%	31%	2%
Medical/BioTech	70%	27%	3%
Military	97%	3%	0%
Other	82%	14%	4%
OVERALL	**76%**	**20%**	**4%**

Attachment 1

Issue Paper: People Barrier’s to Information Assurance

Table 3: Are Budgets Keeping Up?

At your organization, is the budget for infosecurity sufficient?

Industry	Yes	No
Aerospace	33%	67%
Banking/Financial	35%	65%
Communications/Telecom	24%	76%
Consulting	40%	60%
Education	18%	82%
Government	26%	74%
High-Tech/Computer	47%	53%
Insurance/Real Estate/Legal	41%	59%
Manufacturing/Distribution	26%	74%
Medical/BioTech	40%	60%
Military	38%	62%
Other	37%	63%
OVERALL	**34%**	**66%**

Table 4: Organizational Awareness

At your organization, do upper management and end-users support infosecurity needs?*

Industry	Mgmt.	Users
Aerospace	92%	67%
Banking/Financial	83%	54%
Communications/Telecom	83%	54%
Consulting	89%	70%
Education	75%	45%
Government	84%	54%
High-Tech/Computer	85%	60%
Insurance/Real Estate/Legal	84%	50%
Manufacturing/Distribution	64%	40%
Medical/BioTech	83%	57%
Military	78%	47%
Other	83%	53%
OVERALL	**83%**	**55%**

- % indicating "Yes" for each category.

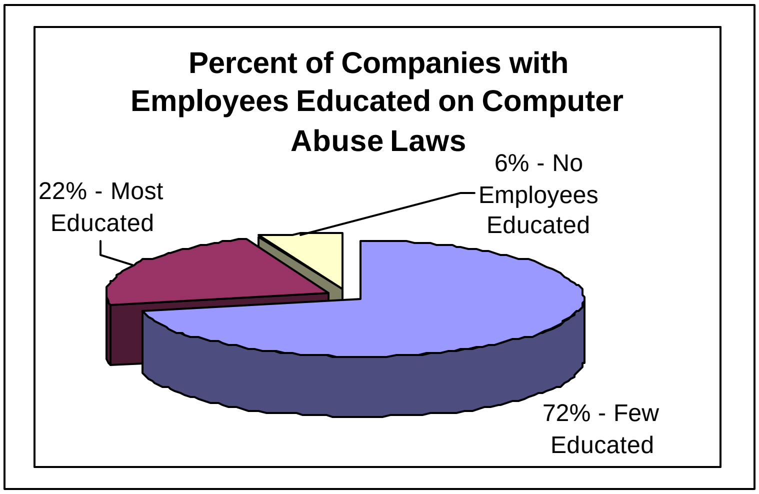

Figure 1. Survey of Federal Agencies and Private Companies Employee Education on Computer Abuse
Source: Computer Security Issues & Trends, Spring 1996

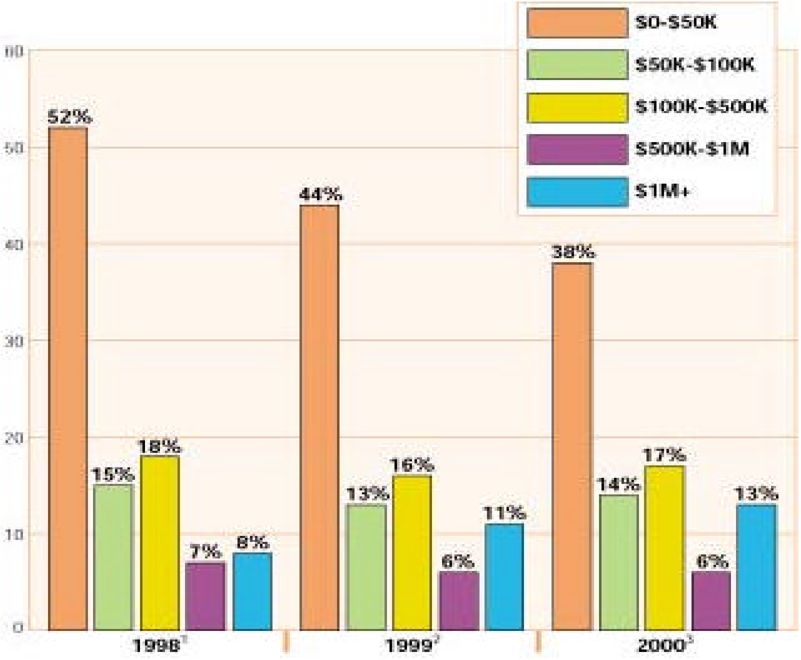

Figure 2: Industry InfoSecurity Budget Growth
Organizational budgets, by year

1. 1998 statistics reflect 1998 Information Security Industry Survey results (www.infosecuritymag.com/industry.htm)
2. Overall results for 1999 do not include 9% of respondents who didn’t answer the question.
3. Overall results for 2000 are projected, and do not include 13% of respondents who didn’t answer the question.

Attachment 2

Issue Paper: People Barrier's to Information Assurance

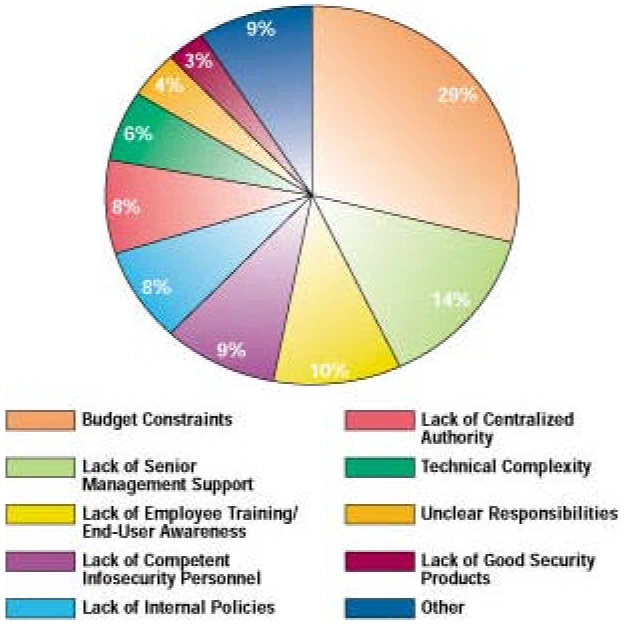

Figure 3: Top Obstacle is Budget
What is the SINGLE greatest obstacle to achieving adequate infosecurity at your organization?

Attachment 2